Troubleshoot email delivery problems and email delivery status notification failures

Helpdesk Reports - 2023-05-21 - Hosted Exchange

Overview:

Mail reputation is important in ensuring the deliverability of emails for all our customers. Furthermore, as a secure data centre and service provider, it is also important in combating the proliferation of spam, viruses and Mmalware over the internet. Micron21 scans all outbound emails for these common issues and threats using our Cisco IronPort Enterprise mail protection platform.

Common Error Codes:

If you have received a Micron21 Email Delivery Status Notification (Failure) message, then it is due to our platform blocking an email (also known as a bounce) based on one of the three reasons below:

- **5.x.0 error message**: The email content contains or resembles spam.
- **5.1.2 bad destination host**: This is where the intended email destination (receiver) contains a domain name which does not have a MX record and therefore cannot receive mail (Note: typically the domain name has been misspelt).
- **5.2.3 error messages:** This is where your email has been detected to contain a virus or malware.

If you are receiving 5.x.0 error messages please read the following information:

The most common error code detected is 5.x.0 due to the prevalence of spam. If you have received this error code, then our mail protection platform has detected spam or something that resembles this. If you sent a legitimate email, then occasionally, these platforms will trigger on what is know as a “false positive”, that is, a genuine email has been treated as spam. The simplest way to address this is to change the content (including potential images or attached filenames) within the email or remove keywords or phrases that may resemble something in a spam email. Most mail protection platforms, including Cisco, safeguard the intellectual property on their detection algorithms. Unfortunately, this means that Micron21 cannot assist in identifying what words may be triggering the detection or in changing your content.

Frequently Asked Questions:

Why are my emails being blocked now, they used to work fine?

Mail protection platforms, such as Micron21’s Cisco IronPort, are continuously improving their technology and spam detection algorithms to deal with the new and evolving methods in which spam content creators attempt to thwart them.

The downside to this forever-changing landscape, is that an email or even a web form which sent fine today, might not send fine tomorrow due to the algorithms treating new content as potential spam.

The only way to resolve this issue is to change the content or images, or attachments, or subject within your email to make it seem less like spam. This may need to be a trial and error process in some cases to determine what works and what gets blocked. As an example, the below two sentences show a subject line that was blocked, then with the removal of the word “full” and some context, was then allowed:

Just ask and we’ll give you a full refund, no questions asked. (BLOCKED)

Just ask and we'll refund your course fee, no questions asked. (ALLOWED)

Other common reasons that emails are being blocked include: attachments; email signatures; or content construction such as: embedded image file names; the amount of capital letters contained within the email; or even that the email itself might be regarded as being simply too basic (i.e. not enough content).

Regardless of the reason, emails that are bouncing with 5.x.0 error messages are doing so - because to our mail protection platform - they look like spam. This may be as simple as changing some basic words or adding more context, or to looking into how the emails are constructed. If you are receiving these messages out of the blue, then it may be due to more nefarious issues such as a vulnerability exploit.

Can Micron21 tell me why my emails are being blocked, or what content is being detected as spam?

Unfortunately no. We can only inform you that it has been bounced due to being detected as Spam, we cannot tell you why or what triggered it to be detected as Spam.

Can Micron21 whitelist emails which I am sending?

Whitelisting is not a practical solution for outbound emails as a feature. If an account is compromised, then mail protection would not work on these whitelisted domains. This inevitably, results in our mail services becoming black listed and then no one could receive any email routed via Micron21.

Why does Micron21 scan outbound emails?

Micron21 scans outbound emails for spam and malware to help keep the internet "clean" and make sure our mail services are not blacklisted. This in turn helps guarantee email deliverability for all legitimate mail originating from Micron21, aiding all our customers.

- Tags
- email
- mail
- troubleshoot